U.S. Government tenants, provided the building is under 24-hour control by U.S. Government personnel.

(3) At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants nor under host government control, provided the classified material is stored in security containers approved by the GSA and is placed under 24-hour control by U.S. Government personnel.

(4) At a U.S. Government activity located in a building not used exclusively by U.S. Government tenants but which is under host government control, provided the classified material is stored in GSA-approved security containers which are further secured in a locked room or area to which only U.S. personnel have access.

(5) When host government and U.S. personnel are co-located, U.S. classified material that has not been authorized for release to the host government pursuant to DoD Directive 5230.11, shall, to the extent possible, be segregated from releasable classified material to facilitate physical control and prevent inadvertent compromise. However, U.S. classified material that is releasable to the host country need not be subject to the 24-hour U.S. control requirement provided the host government exercises its own control measures over the pertinent areas or containers during non-duty hours.

(6) Foreign nationals shall be escorted while in areas where nonreleasable U.S. classified material is handled or stored. However, when required by operational necessity, foreign nationals may be permitted, during duty hours, unescorted entry to such areas provided the nonreleasable information is properly stored or is under the direct personal supervision and control of cleared U.S. personnel who can prevent unauthorized access.

§ 159a.39 Activity entry and exit inspection program.

(a) *Policy*. (1) Commanders and heads of activities shall establish and maintain an inspection program to deter and detect unauthorized introduction or removal of classified material from DoD owned or leased installations and facilities. This program does not replace existing programs for facility and installation security and law enforcement inspection requirements.

(2) The inspection program shall be implemented in a manner which does not interfere unduly with the performance of assigned missions.

(3) The inspection program shall be implemented in a manner which does not significantly disrupt the ingress and egress of persons who are employees of, or visitors to, defense installations and facilities.

(4) Inspections carried out under this program shall be limited to the extent feasible to areas where classified work is being performed, and cover only persons employed within, or visiting, such areas.

(5) Inspections carried out under this program shall be performed at a sufficient frequency to provide a credible deterrent to those who would be inclined to remove classified materials without authority from the installation or facility in question.

(6) The method and frequency of such inspections at a given installation or facility is at the discretion of the commander or head of the installation or facility, or other designated official. Such inspections shall conform to the procedures set forth in the following:

(i) *Inspection Frequency*. (A) Inspections may be aperiodic, that is, at irregular intervals.

(B) Inspections may be accomplished at one or more designated entry/exit points; they need not be carried out at all entry/exit points at the same time.

(C) Inspections may be done on a random basis using any standard which may be appropriate, for example, every third person; every tenth person; every hundredth person, at the entry/exit point(s) designated.

(D) Inspections at a particular entry/exit point(s) may be limited as appropriate to various periods of time, for example, one week, one day, or one hour.

(E) Inspections shall be conducted at all entry/exit points after normal duty hours, including weekends and holidays, on a continuous basis, if practicable.

(b) *Inspection Procedures and Identification*. (1) Inspections shall be limited to that which is necessary to determine whether classified material is

contained in briefcases, shoulder or handbags, luggage, athletic bags, packages, or other similar containers being removed from or taken into the premises. Inspections shall not be done of wallets, change purses, clothing, cosmetic cases, or other objects of an unusually personal nature.

(2) DoD Components shall provide employees who have a legitimate need to remove classified material from the installation or activity with written or printed authorizations to pass through designated entry/exit points. (See §159a.59(f)) This may include:

(i) The authorization statements prescribed in §159a.59.

(ii) If authorized in Component instructions, wallet-size cards which describe in general terms the purpose(s) for authorizing the employee to remove classified material from the facility (for example, use at meetings or transmission to authorized recipients).

(3) Inspectors are to ensure that personnel are not removing classified material without authorization. Where inspectors determine that individuals do not appear to have appropriate authorization to remove classified material, they shall request such individual to obtain appropriate authorization before exiting the premises. If, due to the circumstances, this is not feasible, the inspector should attempt to verify by telephone the authority of the individual in question to remove the classified material with the employing office. When such verification cannot be obtained, and if removal cannot be prevented, the inspector shall advise the employing office and appropriate security office as soon as feasible that classified material was removed by the named individual at a particular time and without apparent authorization.

(4) If the employing office determines that classified material was removed by one of its employees without authority, it shall request an investigation of the circumstances of the removal by appropriate investigative authorities. Where such investigation confirms a violation of security procedures, other than espionage or deliberate compromise, for which §159a.50 applies, appropriate administrative, disciplinary, or legal action shall be taken.

Subpart G—Compromise of Classified Information

§159a.41 Policy.

Compromise of classified information presents a threat to the national security. Once a compromise is known to have occurred, the seriousness of damage to U.S. interests must be determined and appropriate measures taken to negate or minimize the adverse effect of such compromise. When possible, action also should be taken to regain custody of the documents or material that were compromised. In all cases, however, appropriate action must be taken to identify the source and reason for the compromise and remedial action taken to ensure further compromises do not occur. The provisions of DoD Instruction 5240.4[23] and DoD Directive 5210.50[24] apply to compromises covered by this subpart.

§159a.42 Cryptographic and sensitive compartmented information.

(a) The procedures for handling compromises of cryptographic information are set forth in NACSI 4006 and implementing instructions.

(b) The procedures for handling compromises of SCI information are set forth in DoD TS–5105.21–M–2[25] and DoD C–5105.21–M–1[26].

§159a.43 Responsibility of discoverer.

(a) Any person who has knowledge of the loss or possible compromise of classified information shall immediately report such fact to the security manager of the person's activity (see §159a.93(e)) or to the commanding officer or head of the activity in the security manager's absence.

(b) Any person who discovers classified information out of proper control shall take custody of such information and safeguard it in an appropriate manner, and shall notify immediately an appropriate security authority.

[23] See footnote 1 to §159a.3.

[24] See footnote 1 to §159a.3.

[25] See footnote 13 to §159a.33(j).

[26] See footnote 13 to §159a.33(j).